549892

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年9 月30 日 (30.09.2004)

PCT

(10) 国際公開番号
WO 2004/084063 A1

(51) 国際特許分類[7]: G06F 9/06, 15/00

(21) 国際出願番号: PCT/JP2004/003520

(22) 国際出願日: 2004 年3 月17 日 (17.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-072371 2003 年3 月17 日 (17.03.2003) JP

(71) 出願人 (米国を除く全ての指定国について): セイコーエプソン株式会社 (SEIKO EPSON CORPORATION) [JP/JP]; 〒1630811 東京都新宿区西新宿二丁目４番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 黒田 直人 (KURODA, Naoto) [JP/JP]; 〒3928502 長野県諏訪市大和三丁目３番５号 セイコーエプソン株式会社内 Nagano (JP).

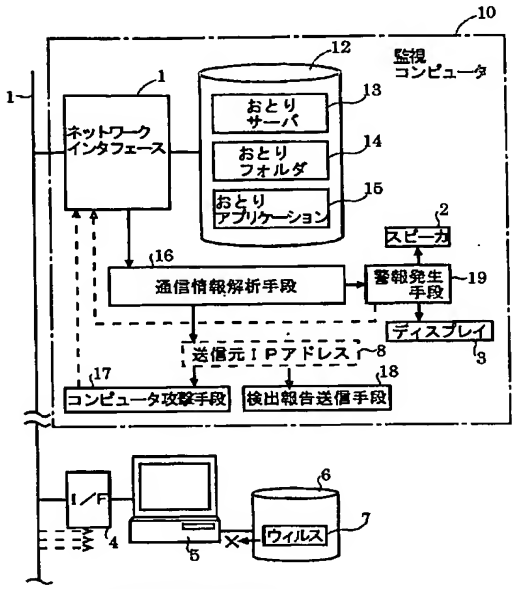
(74) 代理人: 特許業務法人 湘洋内外特許事務所 (THE PATENT CORPORATE BODY SHOWYOU INTERNATIONAL); 〒2200004 神奈川県横浜市西区北幸二丁目９-１０ 横浜ＨＳビル７階 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: METHOD AND SYSTEM FOR PREVENTING VIRUS INFECTION

(54) 発明の名称: ウィルスの感染を阻止する方法およびシステム




1...NETWORK INTERFACE
13...DECOY SERVER
14...DECOY FOLDER
15...DECOY APPLICATION
10...MONITORING COMPUTER
2...LOUDSPEAKER
16...COMMUNICATION INFORMATION ANALYSIS MEANS
19...ALARM GENERATION MEANS
3...DISPLAY
8...SOURCE IP ADDRESS
17...COMPUTER ATTACK MEANS
18...DETECTION REPORT TRANSMISSION MEANS
7...VIRUS

(57) **Abstract:** There is disclosed a system for detecting virus infection in a network and preventing the virus infection. Decoy means (13, 14, 15) accessible via the network (1) are arranged on a storage device (12). The system includes: communication information analysis means (16) for detecting virus intrusion into the decoy means (13, 14, 15) and upon detection of the virus intrusion, detecting a computer as a source of the virus from the communication information acquired upon the virus intrusion; and computer attack means (17) for performing virus attack process to the virus source computer for suppressing action of the virus via the network. Attack of the computer attack means (17) by a monitoring computer (10) is continued until a computer (5) infected with virus is identified and the virus is removed by an administrator.

(57) 要約: ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムが開示される。ネットワーク（１）を介してアクセスが可能なおとり手段（１３，１４，１５）が記憶装置（１２）上に設けられる。おとり手段（１３，１４，１５）へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段（１６）と、ウィルス送信元コンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段（１７）と、を備える。ウィルスに感染しているコンピュータ（５）を特定し、管理者がウィルスを除去する等の対策を終了するまでの間、監視コンピュータ（１０）のコンピュータ攻撃手段（１７）による攻撃を行う。

WO 2004/084063 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

# 明　細　書

## ウィルスの感染を阻止する方法およびシステム

### 技術分野

本発明は、ネットワークに接続されたコンピュータがウィルスに感染したとき、感染源を突き止めて、同じネットワークに接続された他のコンピュータへの感染を阻止する技術に関する。

### 背景技術

コンピュータウィルスには、サーバ等のコンピュータの共有フォルダに侵入して、所定のファイルやプログラムにアクセスをし、それを破壊したり、誤動作させるように書き換えたりするものがある。ウィルスの存在は、所定のプログラムを使って検出することができる。このプログラムは、ウィルスのファイル名、ウィルスの行動パタン等から、ウィルスであると判断をする。ウィルスを検出すると、コンピュータの管理者は必要な処置を施し、ウィルスを除去する。ウィルスを検出してワクチンを配布する技術は、各種紹介されている（特許文献１：特開２００２－２５９１４９号公報参照）。

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

ウィルスを検出したときは、すみやかにその存在場所を突き止めて、ネットワークから切離し、ワクチンを用いて駆除するという処理をしなければならない。しかしながら、ウィルスを検出してから対策処理を完了するまでの間に時間がかかる場合がある。時間がかかると、次々と被害が拡大して、ネットワークに重大な被害を及ぼす恐れもある。

また、ネットワーク上の別のコンピュータに潜んで、ネットワークを

通じてファイルアクセスをしてくるようなウィルスは、活動を開始するまで検出が困難なことがある。そのウィルスが活動を開始し、ウィルスを検出したとしても、ウィルスの潜んでいるコンピュータを調べて、そのウィルスを駆除するまで時間がかかると、被害が拡大するという問題があった。

## 発明の開示

本発明は、ネットワークに接続されたコンピュータがウィルスに感染していることを突き止めると共に、同じネットワークに接続された他のコンピュータへの被害の拡大を阻止する技術を提供することを目的とする。

本発明の第１の態様によれば、

ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止する方法であって、

ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、そのおとりにウィルスが侵入したとき、対応して取得した通信情報に基づいて、ウィルスの送信元となっているコンピュータを検出し、ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うこと、を特徴とするウィルスの感染を阻止する方法が提供される。

本発明の第２の態様によれば、

ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ネットワークを介してアクセスが可能なおとり手段と、

前記おとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルス

の送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステムが提供される。

本発明の第３の態様によれば、

ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことについての依頼を受ける手段と、

前記受けた依頼に基づいて、前記ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステムが提供される。

本発明の第４の態様によれば、

ネットワークでのウィルスの感染を検出して、ウィルスの感染の阻止をコンピュータに実行させるプログラムであって、

予め設けられたネットワークを介してアクセスが可能なおとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、をコンピュータに構築させる、ウィルスの感染を阻止するプログラムが提供される。

また、本発明の第５の態様によれば、

ネットワークでのウィルスの感染を検出して、ウィルスの感染の阻止をコンピュータに実行させるプログラムであって、

ウィルスの送信元となっているコンピュータネットワークアドレスの

通知を受けたとき、ウィルスの送信元となっているコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウィルスの感染を阻止するプログラムが提供される。

## 図面の簡単な説明

図１は、ウィルスの感染を阻止するシステムの具体例を示すブロック図である。

図２は、検出報告の例を示す説明図である。

図３は、複数のコンピュータにより感染コンピュータを攻撃する例を示す説明図である。

図４は、大規模なコンピュータネットワークの説明図である。

図５は、監視コンピュータの基本動作を示すフローチャートである。

図６は、監視コンピュータの協力動作を示すフローチャートである。

## 発明を実施するための最良の形態

以下、発明を実施するための最良の形態について、その原理を含む概要について説明する。その後、詳細について説明する。

ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ（監視コンピュータ）上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、そのおとりにウィルスが侵入したとき、対応して取得した通信情報に基づいて、ウィルスの送信元となっているコンピュータを検出し、ウィルス送信元コンピュータ（感染コンピュータ）に対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行う。また、ウィルスの送信元となっているコンピュータの管理者宛に検出報告を送信する。

ここで、おとりには、セキュリティが低いものを用意して、ウィルスの侵入を促す。おとりのセキュリティを低くするには、ウィルスからの保護を想定している各種コンピュータにおけるセキュリティより、低くすることにより実現する。ただし、他のコンピュータよりセキュリティが低いかを調べることは必ずしも容易ではない。そこで、ウィルス対策の程度によって、セキュリティの差を付けることが考えられる。例えば、一般的に行うべきウィルス対策を全く採らないことが考えられる。具体的には、ウィルス対策ソフトウェアをインストールしないこと、または、インストールされているウィルス対策ソフトウェアを無効とすること、オペレーティングシステム、アプリケーション等に、セキュリティホールがある場合には、そのまま放置すること等が挙げられる。

なお、このウィルス対策を、特定のコンピュータ群のために行う場合には、対象となるコンピュータのセキュリティレベルが既知であることが多い。このような場合、対象となるコンピュータ群の中で、セキュリティの最も低いコンピュータより低いセキュリティとなるように、おとりのセキュリティを設定する。このようにすることで、おとりを、ウィルス対策を行うべきコンピュータ群の中で最もウィルスに侵入され易くすることができる。

おとりとしては、例えば、図１に示すように、おとりフォルダ１４を設けること、おとりアプリケーション１５を設けること、おとりサーバ１３を設けること等が挙げられる。これらを単独で、または、２以上を併用することができる。おとりを複数のコンピュータに分散して設けることもできる。

おとりフォルダ１３は、ネットワーク１に接続されたコンピュータ１０の記憶装置１２上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成することができる。フォルダにおけるウィルスの侵入とは、ウィルスが、ネットワークを通じて、フォルダ中の任意のファイルを読み出したり、ファイルの書き替えを試みたりする状況をいう。ウィルスに感染するというのは、ウィルス自体がコンピュータ

の記憶装置のどこかに取り込まれていることをいう。

通信情報は、ウィルスがおとりフォルダに侵入をしたときにネットワークから受信した通信経路等の情報である。この通信情報中に、ウィルスの送信元となっているコンピュータのネットワークアドレス等が含まれる。ウィルスの送信元となっているコンピュータは、ウィルスに感染したコンピュータである。おとりフォルダで待ち受けるので、侵入してきたウィルスを検出できる。検出報告の内容は任意である。報告方法も任意である。感染したコンピュータの管理者に通知すると同時にその感染源のコンピュータを攻撃する。

探索の対象となるウィルスが、共有フォルダへ侵入する性質を持つウィルスであることもある。このような共有フォルダへ侵入するウィルスは、おとりフォルダを設けることで、その活動を検出できる。

おとりアプリケーション１５は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成される。このおとりは、サーバへ侵入する性質を持つウィルス検出のための構成である。おとりフォルダの代わりにおとりアプリケーションを設けた例である。例えば、探索の対象となるウィルスがアプリケーションの誤動作を引き起こす性質を持つウィルスである場合、擬似的なおとりアプリケーションを設けることで、その活動を検出できる。

おとりサーバ１３は、サーバへ侵入する性質を持つウィルスを検出する。おとりサーバは、擬似的なアプリケーションにより構成され、みかけ上サーバの構成を持つデータを有する。おとりサーバ１３は、それに対してアクセスがあると、そのアクセスに対してサーバと同様の応答を返す機能を持つ。想定されるサーバの形式は、アクセスの対象となるサーバであればよい。例えば、ウェブサーバ、メールサーバ等がある。いずれであってもよい。このおとりサーバは、サーバ攻撃型のウィルスに対応するための構成である。コンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に、おとりフォルダを設けた構成としているので

、ウィルスの攻撃を受けてもその影響を受けない。すなわち、被害は発生しない。同時に、攻撃を受けながら、その出所を突き止めることができる。おとりサーバとおとりフォルダとは、全く別のものでも、一体化したアプリケーションにより構成されるものでもよい。

おとりに、ウィルスが侵入をしたとき、直ちに感染源を突き止めて、被害の拡大を阻止した上で対策を施す。すなわち、感染コンピュータに対し、ウィルスの活動を抑制するウィルス攻撃処理を行う。ウィルス攻撃処理としては、高負荷を与えるための情報を、ネットワークを介して送信することが挙げられる。攻撃は、ウィルスの駆除が完了するまで継続する。ウィルス対策とは、感染コンピュータをネットワークから切り離すこと、または、ウィルスを駆除することである。

主体から見た攻撃態様としては、単独攻撃、依頼攻撃、共同攻撃等がある。単独攻撃は、監視コンピュータが、単独で感染コンピュータを攻撃するものである。依頼攻撃は、監視コンピュータが、感染コンピュータの近くに所在する、攻撃能力を有するコンピュータに攻撃を依頼して、依頼されたコンピュータが感染コンピュータを攻撃するものである。共同攻撃は、複数のコンピュータにより感染コンピュータを攻撃するものである。これらの詳細については後述する。なお、依頼攻撃の際の攻撃方法、共同攻撃の場合の攻撃方法は、監視コンピュータが定めて、統一的に攻撃するようにすることができる。また、依頼先、共同の相手先の各コンピュータが有する攻撃能力に基づいて攻撃するよう依頼することもできる。

また、攻撃の内容としては、本発明では、前述したように、感染コンピュータにおいてウィルスの活動を抑圧するため、または、感染コンピュータ中のウィルスの活動を阻止するため、感染コンピュータに対して高い通信負荷をかける方法と、感染コンピュータのＣＰＵに高い負荷をかける方法とを用いる。いずれか一方、または、両者を組み合わせて用いてもよい。攻撃の仕方の詳細については後述する。

ウィルスの送信元となっている感染コンピュータを検出した場合、ま

ず、感染コンピュータの管理者宛の検出報告を発する。その上で、当該ウィルスへの対策が完了するまで攻撃を行う。

また、感染コンピュータを攻撃するに当たり、攻撃開始を予告するための、メッセージを送信して、コンピュータの使用者、管理者に注意を促す。さらに、攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生させる。これにより、感染コンピュータとネットワークを共有している他の端末装置の使用者に注意を促すことができる。警報音の種類は任意である。また、ディスプレイに攻撃動作中の表示をしてもよい。

攻撃を行うため、監視コンピュータはもとより、依頼先のコンピュータ、共同攻撃に参加するコンピュータには、それぞれウィルスの送信元となっているコンピュータに負荷を与える処理を当該コンピュータに実行させるための攻撃プログラム（ウィルス対策プログラム）を持たせておく。このウィルス対策プログラムを、必要に応じて監視コンピュータから、適宜、他のコンピュータにインストールする構成としてもよい。

また、監視コンピュータ以外の攻撃に参加するコンピュータは、攻撃機能を有すれば足りる。従って、監視機能を持っていなくてもよい。

一方、感染コンピュータ以外のコンピュータの防御策も用意しておく。例えば、ウィルスの送信元となっているコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となっているコンピュータからの通信を拒絶する処理を、コンピュータに実行させる。また、ネットワーク監視用のコンピュータから、感染コンピュータの通知を受けたとき、防御のためにウィルスの送信元となっているコンピュータからの通信を拒絶する処理を実行する。

次に、本発明の実施の形態について、それぞれ図面を参照して説明する。

図１は、ウィルス対策システムの具体例を示すブロック図である。ネットワーク１には、ネットワークインタフェース４を介してコンピュータ５が接続されている。このコンピュータ５には、記憶装置６が設けら

れている。この記憶装置６に、ウィルス７が感染しているものとする。このコンピュータ５を感染コンピュータと呼ぶことにする。

ネットワーク１には、監視コンピュータ１０が接続されている。監視コンピュータ１０は、ネットワークインタフェース１１と、記憶装置１２とを備える。記憶装置１２には、おとりサーバ１３と、おとりフォルダ１４と、おとりアプリケーション１５とが記憶されている。コンピュータ１０は、それが実現する機能として、ネットワークインタフェース１１で取得される通信情報を監視するために、通信情報解析手段１６が設けられている。通信情報解析手段１６の出力は、警報発生手段１９を駆動する。さらに、通信情報解析手段１６の出力に基づいて、コンピュータ攻撃手段１７と検出報告送信手段１８とが動作するように構成されている。通信情報解析手段１６とコンピュータ攻撃手段１７と検出報告送信手段１８と警報発生手段１９とは、いずれも、コンピュータ１０の図示していないＣＰＵにより実行されて、監視コンピュータ１０に所定の処理を実行させるコンピュータプログラムである。これらのプログラムは、記憶装置１２にインストールされ、実行時に図示していないＣＰＵにロードされる。

この発明は、ウィルス７に感染しているコンピュータ５を特定し、そのコンピュータ５の管理者がウィルス７を除去するまでの間、そのコンピュータ５に高負荷を生じさせ、ウィルス７の活動を抑制する。ウィルス７に感染しているコンピュータ５を特定するために、おとりサーバ１３、おとりフォルダ１４およびおとりアプリケーション１５をネットワーク１中に構築する。おとりサーバ１３等は、監視コンピュータ１０中に擬似的に生成する。おとりフォルダ１４は、監視コンピュータ１０の記憶装置１２中の、任意の場所に生成するとよい。また、おとりサーバ１３中に一体に生成する。

［おとりサーバ等］

おとりのサーバ１３は、ネットワーク１上で最先にウィルス７が攻撃してくるような環境となるように環境設定を行うことが好ましい。セキ

ュリティのレベルを最も低くするとともに、例えば、コンピュータ名は、ネットワークコンピュータリストの最も上位に表示されるような名称に選定する。また、ウィルスを受け入れるための共有フォルダ名は、ウィルスがアタックしやすい性質のフォルダ名とする。これも、共有フォルダリストの最も上位に表示されるような名称に選定するとよい。また、コンピュータ名もフォルダ名も、ウィルスの性質から最適なものを決定するとよい。例えば、おとりサーバ１３は、ウィルス７が実在のサーバに対して侵入を試みた場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のサーバとは異なるから、破壊活動に対しては何の影響もない。例えば、フォルダ１４は、ウィルス７が実在のフォルダに対してアクセスした場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のフォルダとは異なるからファイルの削除といった破壊活動に対して何の影響もない。おとりアプリケーション１５は、実際のアプリケーションとは異なるから、誤動作を引き起こされる恐れはない。

［感染コンピュータの特定］

通信情報解析手段１６には、ウィルスの侵入を検出すると、直ちにその通信情報中から発信源のコンピュータ名を解析して、特定する機能を持つ。この情報には、誰がログオンしたコンピュータか、そのコンピュータのアドレスは何か、コンピュータを使用している社員の社員コードは何か、といった情報が含まれる。

なお、コンピュータウィルスを発見した場合に、感染しているコンピュータを、無条件で直ちに攻撃すると、使用者がとまどって様々な弊害が生じる。そこで、警報発生手段１９を設ける。警報発生手段１９は、例えば、ポップアップメッセージなどの通知手段を使って、感染コンピュータに対し、「このコンピュータはウィルスに感染しています。早急にネットワークから切り離してください」といった対策開始を予告するメッセージを送信する機能を持つ。さらに、周辺のコンピュータ利用者に対し、ネットワークを通じて、ウィルス７が侵入する恐れがある旨の

警告を発するために、例えば、スピーカ２を鳴らしたりディスプレイ３に警報画面を表示したりする機能を持つ。

図２（ａ）および図２（ｂ）は、検出報告の例を示す説明図である。通信情報解析手段１６（図１参照）は、通信情報から取得した送信元ＩＰアドレス８を検出報告送信手段１８に転送する。検出報告送信手段１８は、感染コンピュータ５の管理者に対して、例えば、電子メールやファクシミリを利用して、検出報告を送信する。図２（ａ）は拡散型のウィルスを検出したときの検出報告例である。図２（ｂ）は、ネットワーク共有型のウィルスを検出したときの検出報告例である。例えば、図２（ａ）では、ＩＰアドレスが「192.168.10.15」のコンピュータに、同図のようなパタンのウィルスによる攻撃がされている。といった報告である。

［ウィルスの侵入と感染コンピュータの検出］

ウィルスが、ネットワーク上のいずれかのコンピュータに取り込まれると、所定のタイミングで活動を開始する。例えば、ウィルスは、ネットワークを通じて他のコンピュータの共有フォルダをアクセスして、そこに格納されたファイルを書き換えたり、破壊したりする。ウィルスが侵入するというのは、このように、共有フォルダをアクセスする行為のことをいう。ウィルスファイルが実際にコピーされるとは限らない。従って、ウィルスが侵入されたコンピュータでは、通常の状態では、ウィルスの侵入によるファイルのアクセスか、正常なファイルのアクセスかを区別できず、ウィルスを検出できないこともある。

そこで、おとりサーバ、および、おとりフォルダを設ける。通常のアプリケーションは、予め特定したサーバ、または、フォルダにのみアクセスする。擬似的に作成された、おとりサーバまたはおとりフォルダにアクセスするのは、ウィルスである確率が極めて高い。さらに、そのアクセスパターンを確認することで、ウィルスであるとの確証を得ることができる。その後は、その通信情報から、どのコンピュータがそのウィルスに感染したかを突き止める。感染コンピュータでのウィルスの活動

を阻止しなければ、このウィルスがネットワークを通じて様々なコンピュータに被害を及ぼす。

［感染コンピュータに対する攻撃］

コンピュータ攻撃手段１７（図１）は、感染コンピュータに対して所定の攻撃動作をする機能を持つ。このコンピュータ攻撃手段１７は、感染コンピュータ５に対して、高い負荷をかける。感染コンピュータ中のウィルスの活動を阻止するためであるから、感染コンピュータ５に対して高い通信負荷をかける方法と、感染コンピュータのＣＰＵに高い負荷をかける方法がある。

感染コンピュータ５に対して高い通信負荷をかけると、ネットワーク１と感染コンピュータ５との間を結ぶネットワークインタフェース１１等の通信路でトラフィックが増大して、感染コンピュータ５からネットワーク１に対する通信の通信速度が著しく低下する。従って、感染コンピュータ５内部からネットワーク１を経由して他のコンピュータに向かうウィルスの侵入活動が抑制される。具体的には、１００ＢＡＳＥ－Ｔ程度の帯域を持つネットワークならば、５メガバイト程度もある大きなパケットを感染コンピュータ宛に送信するとよい。しかしながら、この場合、ＣＰＵ自体にはさほどの負荷はかからない。

一方、感染コンピュータ５のＣＰＵに高い負荷をかけると、感染コンピュータ５の内部でデータの破壊活動をしようとするウィルスの活動速度が著しく低下する。従って、感染コンピュータ５中にウィルス被害が広がることを防止できる。例えば、Ｐｉｎｇパケットを大量に連続的に送信する。これにより、ＣＰＵが過負荷になるので、コンピュータの内部でのウィルスの活動を阻止し、被害の拡大を抑制できる。具体的には、２バイト程度のＰｉｎｇパケットを感染コンピュータ５に向けて大量に連続的に送信する。感染コンピュータ５のＣＰＵは、パケットを受信する度に応答を返すための制御をしなければならないので、ＣＰＵが過負荷になる。

従って、上記の一方または両方の方法を併用するとよい。もちろん、

上記以外の既知の任意の方法で、感染コンピュータに対して、高い負荷をかけるようにしてもよい。

［複数のコンピュータによる攻撃］

図３は、複数のコンピュータにより、感染コンピュータ５を攻撃する例を示す説明図である。図３のネットワーク１には、監視コンピュータ１０および感染コンピュータ５と、端末装置２０と、端末装置２２と、端末装置２４とが接続されている。端末装置２０は、ネットワークインタフェース２１を介してネットワーク１に接続されている。端末装置２２は、ネットワークインタフェース２３を介してネットワーク１に接続されている。端末装置２４は、ネットワークインタフェース２５を介してネットワーク１に接続されている。

端末装置２０は、コンピュータ攻撃手段３１を備えている。端末装置２２は、コンピュータ攻撃手段３２を備えている。端末装置２４は、コンピュータ攻撃手段３３を備えている。コンピュータ攻撃手段３１、コンピュータ攻撃手段３２およびコンピュータ攻撃手段３３は、いずれも、監視コンピュータ１０のコンピュータ攻撃手段１７と同様の機能を持つ。

１台のコンピュータでは、感染コンピュータを攻撃するのが不十分な場合がある。この場合には、図３に示すように、監視コンピュータ１０は、別のコンピュータ、例えば、端末装置２０、２２および２４に対して、攻撃を依頼する。そして、複数台のコンピュータ１０、２０、２２および２４の協力によって、１台のコンピュータ５を共同で攻撃する。これによって、ウィルスが感染したコンピュータの機能を制限する。一方、その間に、管理者に通知して、ウィルスを削除するための時間を稼ぐ。

端末装置２０等は、攻撃専用のコンピュータでもよいし、一般ユーザの使用しているコンピュータにコンピュータ攻撃手段３１等をインストールしたものでもよい。監視コンピュータ１０は、ネットワーク１中に１台だけ設けること、複数台設けることのいずれであってもよい。

なお、監視コンピュータ１０からコンピュータ攻撃手段３１等に送信する攻撃依頼には、感染コンピュータのＩＰアドレス（ネットワークアドレス）を含める。また、コンピュータ攻撃手段３１等を起動するコマンドを含めるとよい。コンピュータ攻撃手段を持つコンピュータは、監視コンピュータと同様の機能を持つコンピュータでもよいし、攻撃手段のみを持つコンピュータでもよい。

図４は、大規模なコンピュータネットワークの説明図である。図４に示すように、ルータ５０とルータ５１とにより、相互に接続されたネットワーク５２とネットワーク５３とネットワーク５４とには、それぞれ、多数のコンピュータが接続されている。ネットワーク５２に接続されたコンピュータ６１と６２のうち、コンピュータ６２は監視コンピュータである。ネットワーク５３に接続されたコンピュータ６３と６４と６５のうち、コンピュータ６３は監視コンピュータである。ネットワーク５４に接続されたコンピュータ６６と６７と６８のうち、コンピュータ６８は監視コンピュータである。

例えば、コンピュータ６７が感染コンピュータであって、コンピュータ６２がそのウィルスの侵入を検知することがある。このときは、コンピュータ６２から攻撃をしても、ルータ５０やルータ５１がボトルネックになって、効果的な攻撃が難しい。そこで、コンピュータ６２は、コンピュータ６７の所属するネットワーク５４に接続された最寄りのコンピュータ６８に対して、コンピュータ６７への攻撃を依頼する。コンピュータ６８は、先に説明したスピーカ等による警報を発して、周囲のコンピュータ６６等に注意を促してから、コンピュータ６７への攻撃を開始する。こうして、大規模なネットワークにおける監視動作も可能になる。

［動作フローチャート］

図５は監視コンピュータの基本動作を示すフローチャートである。具体的には、監視コンピュータ１０は、プログラムを実行して、各種機能を実現する。それによって、監視コンピュータ１０は、通信情報解析手

段１６、コンピュータ攻撃手段１７、検出報告手段１８および警報発生手段１９として機能する。

まず、監視コンピュータ１０は、おとりサーバ１３、おとりフォルダ１４、および、おとりアプリケーション１５を有効にする初期設定を行う（ステップＳ１）。この状態で、ウィルスの待ち受けを開始する（ステップＳ２）。通信情報解析手段１６は、ネットワークインタフェース１１の処理する通信情報を監視する。

ウィルスの侵入を検知すると、通信情報解析手段１６は、通信情報の解析をして、送信元ＩＰアドレス８を取得し、感染コンピュータを特定する（ステップＳ３、Ｓ４、Ｓ５）。検出報告送信手段１８は、管理者へ検出報告をする（ステップＳ６）。

警報発生手段１９は、スピーカ２による警報音を鳴らす（ステップ７）。また、攻撃中である旨の動画等を、監視コンピュータ１０のディスプレイ３に表示する。さらに、警報発生手段１９は、感染コンピュータ５に対して攻撃開始メッセージを送信する（ステップＳ８）。

コンピュータ攻撃手段１７は、攻撃を開始する（ステップＳ９）。その後、任意のルートでウィルス対策が完了した旨の報告を受けかを判断する（ステップＳ１０）。ウィルス対策が完了した旨の報告を受けた場合、コンピュータ攻撃手段１７による攻撃を終了する（ステップＳ１１）。

図６は、監視コンピュータの協力動作を示すフローチャートである。複数のコンピュータの協力を得て幹線コンピュータの攻撃を行う場合にも、前述した監視コンピュータ１０の各種機能により、感染コンピュータの発見処理と、攻撃協力のための依頼処理と、強調攻撃処理とが行われる。

監視コンピュータ１０は、まず、感染コンピュータを特定する（ステップＳ２１－ステップＳ２４）。この感染コンピュータを特定するための処理は、前述した図５に示す（ステップＳ２－ステップＳ５）の処理と同様である。

感染コンピュータを特定されたら、コンピュータ攻撃手段１７が、ネットワークの調査をする（ステップＳ２５）。最寄りの監視コンピュータを探すためである。最寄りの監視コンピュータを探すには、予め用意した監視コンピュータのリストから、感染コンピュータとＩＰアドレスの一部が共通している監視コンピュータを検索する（ステップＳ２６）。

最寄りの監視コンピュータが、自分自身である場合と、図４で説明したように、ルータのような幾つかのネットワークコンポーネントを介して接続された監視コンピュータである場合とがある。そこで、最寄りの監視コンピュータが自分自身かどうかを判断する（ステップＳ２７）。自分自身でなかったら、攻撃依頼先を決定する（ステップＳ２８）。該当する監視コンピュータが複数ある場合は、複数の監視コンピュータに同報送信で攻撃依頼を発信すればよい。

続いて、該当する監視コンピュータに対して、攻撃依頼の発信をする（ステップＳ２９）。その後は、攻撃依頼先において、図５のステップＳ６以降の処理が実行される。

［感染コンピュータの処置］

感染コンピュータは被害を受けている可能性が高いので、すみやかにネットワークから切り離すことが最も効果的な対策である。この対策が完了すれば、感染コンピュータへの攻撃は終了してよい。

感染コンピュータについては、その後、ウィルスの除去処理をして、被害があった部分を修復する。また、ＯＳ（オペレーティングシステム）、アプリケーション等の再インストールをして復旧させる。このために、図３に示すように、記憶装置６には、その旨のメッセージを含む画面４０をディスプレイに表示する。この画面４０は、必要な対応措置が終了後、ボタン４１がクリックされるまで表示される。

この発明は、ネットワークを通じて拡散するタイプのウィルスの拡散スピードを低下させる機能を持つ。すなわち、ウィルスが感染したコンピュータに大きな負荷をかけることによって、ウィルスの拡散を阻止す

る。また、ウィルスが、あるコンピュータの共有ファイルに侵入しても、その動作だけでは侵入を直ちに確認することができない場合に適する。すなわち、ウィルスが活動したとき、そのウィルスの攻撃を真っ先に受けるようにおとりのコンピュータを設定する。これによって、ウィルスを発見し、ウィルスがどのコンピュータに感染しているかを確認し、該当する攻撃対象のコンピュータを特定する。すなわち、単にフォルダ内に侵入しただけでは、発見の難しいウィルスの検出と排除に有効である。

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウエアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えば、ＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

請求の範囲

1．　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止する方法であって、

ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、そのおとりにウィルスが侵入したとき、対応して取得した通信情報に基づいて、ウィルスの送信元となっているコンピュータを検出し、ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うこと、を特徴とするウィルスの感染を阻止する方法。

2．　請求項1に記載のウィルスの感染を阻止する方法において、

前記おとりは、おとりフォルダを記憶装置に記憶させたもの、おとりアプリケーションを記憶装置に記憶させたもの、および、記憶装置に擬似的に形成したサーバ、のうち1以上であるウィルスの感染を阻止する方法。

3．　請求項1に記載のウィルスの感染を阻止する方法において、

前記ウィルス攻撃は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止する方法。

4．　請求項3に記載のウィルスの感染を阻止する方法において、

前記ウィルスの送信元となっているコンピュータに与える高負荷は、当該コンピュータのトラフィックを増大させることであるウィルスの感染を阻止する方法。

5．　請求項3に記載のウィルスの感染を阻止する方法において、

前記ウィルスの送信元となっているコンピュータに与える高負荷は、当該コンピュータのＣＰＵが応答動作をすべき処理を大量に要求することであるウィルスの感染を阻止する方法。

6．　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ネットワークを介してアクセスが可能なおとり手段と、

前記おとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。

7．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、おとりフォルダを記憶装置に記憶させたもの、おとりアプリケーションを記憶装置に記憶させたもの、および、記憶装置に擬似的に形成したサーバ、のうち１以上であるウィルスの感染を阻止するシステム。

8．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止するシステム。

9．　請求項８に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのトラフィックを増大させて、当該コンピュータ高負荷を与

えることであるウィルスの感染を阻止する方法。

１０．　請求項８に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのＣＰＵが応答動作をすべき処理を大量に要求して、当該コンピュータに高負荷を与えることであるウィルスの感染を阻止するシステム。

１１．　請求項８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段をさらに備え、

前記コンピュータ攻撃手段は、当該ウィルスへの対策が完了するまで、当該コンピュータへの攻撃を継続するウィルスの感染を阻止するシステム。

１２．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成されるおとりフォルダであるウィルスの感染を阻止するシステム。

１３．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成されるおとりアプリケーションであるウィルスの感染を阻

止するシステム。

１４．　請求項８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

感染したコンピュータに対して、高負荷を与える攻撃開始を予告するためのメッセージを送信する手段をさらに備えるウィルスの感染を阻止するシステム。

１５．　請求項８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段をさらに備えるウィルスの感染を阻止するシステム。

１６．　請求項８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

ネットワークに接続された別のコンピュータに対して、ウィルス送信元となっているコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことを依頼する手段をさらに備えるウィルスの感染を阻止するシステム。

１７．　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことについての依頼を受ける手段と、

前記受けた依頼に基づいて、前記ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。

１８．　ネットワークでのウィルスの感染を検出して、ウィルスの感染の阻止をコンピュータに実行させるプログラムであって、

予め設けられたネットワークを介してアクセスが可能なおとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルス送信元コンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段とをコンピュータに構築させる、ウィルスの感染を阻止するプログラム。

１９．　ネットワークでのウィルスの感染を検出して、ウィルスの感染の阻止をコンピュータに実行させるプログラムであって、

ウィルスの送信元となっているコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となっているコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウィルスの感染を阻止するプログラム。

図1

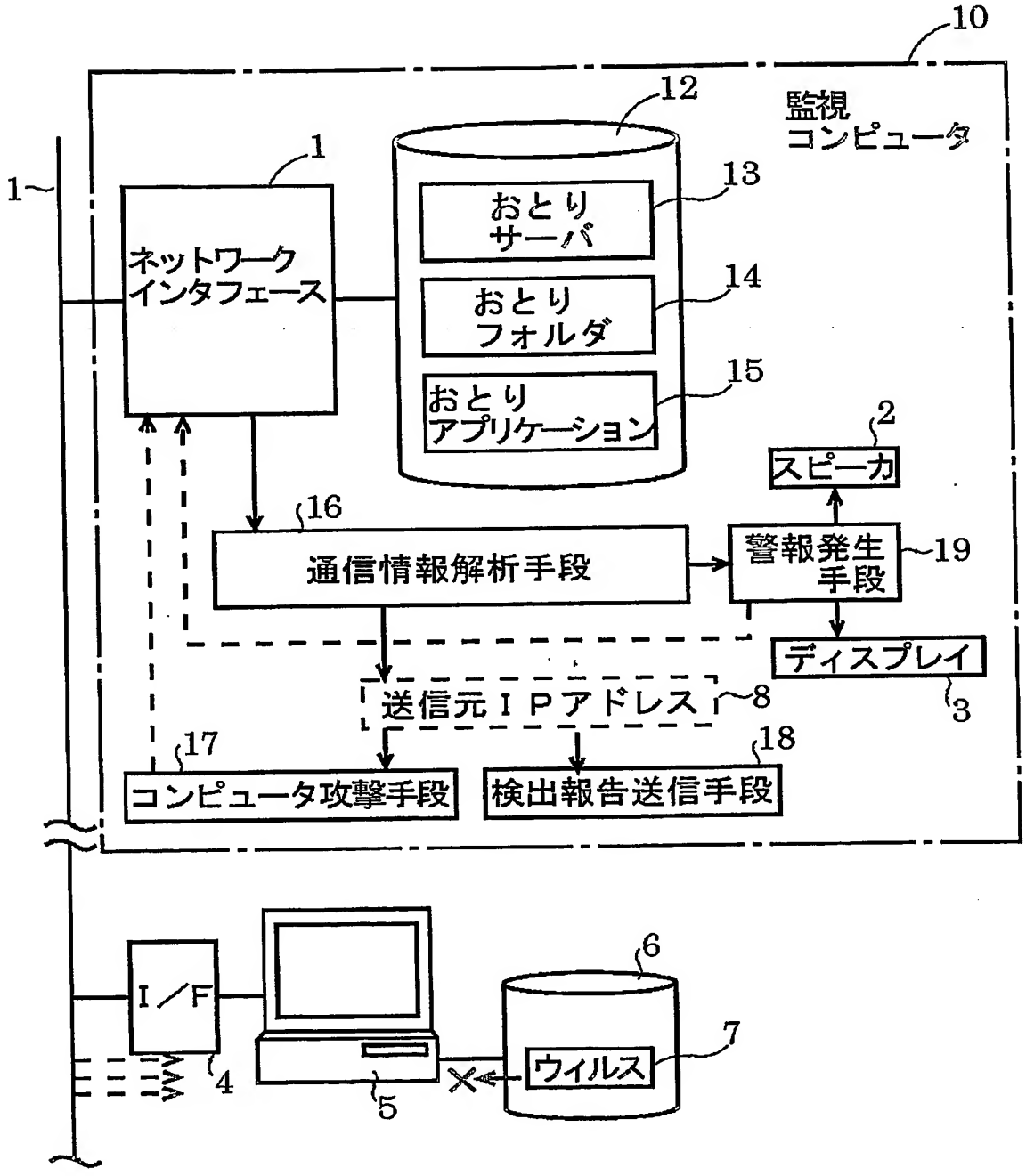
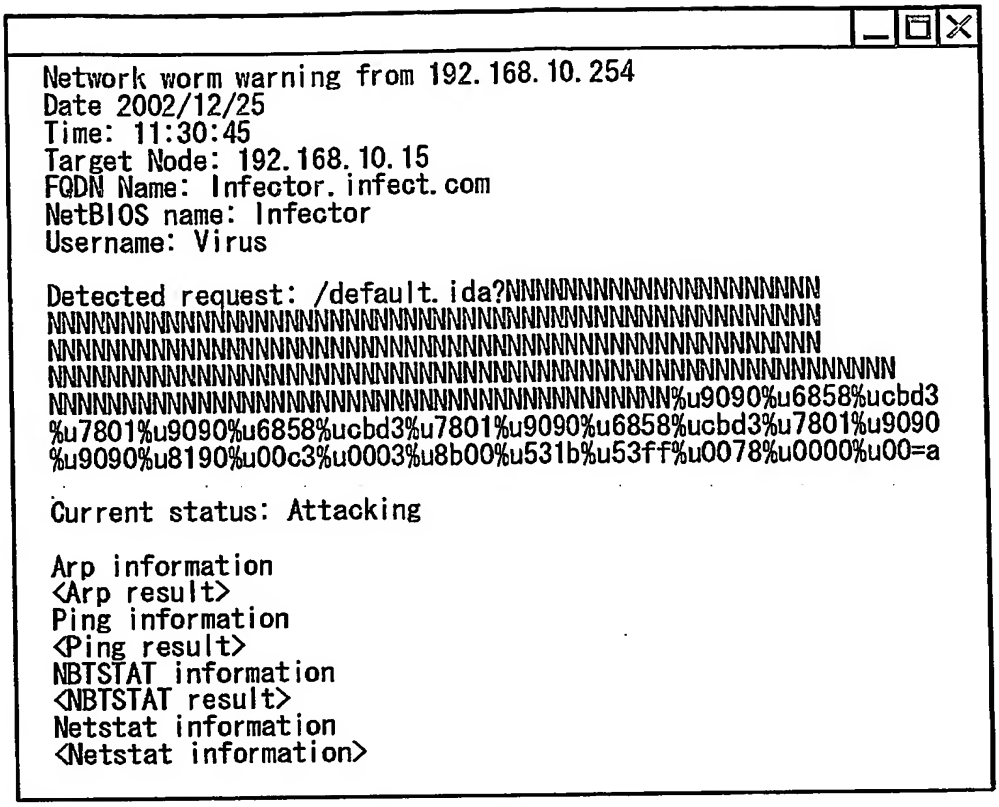
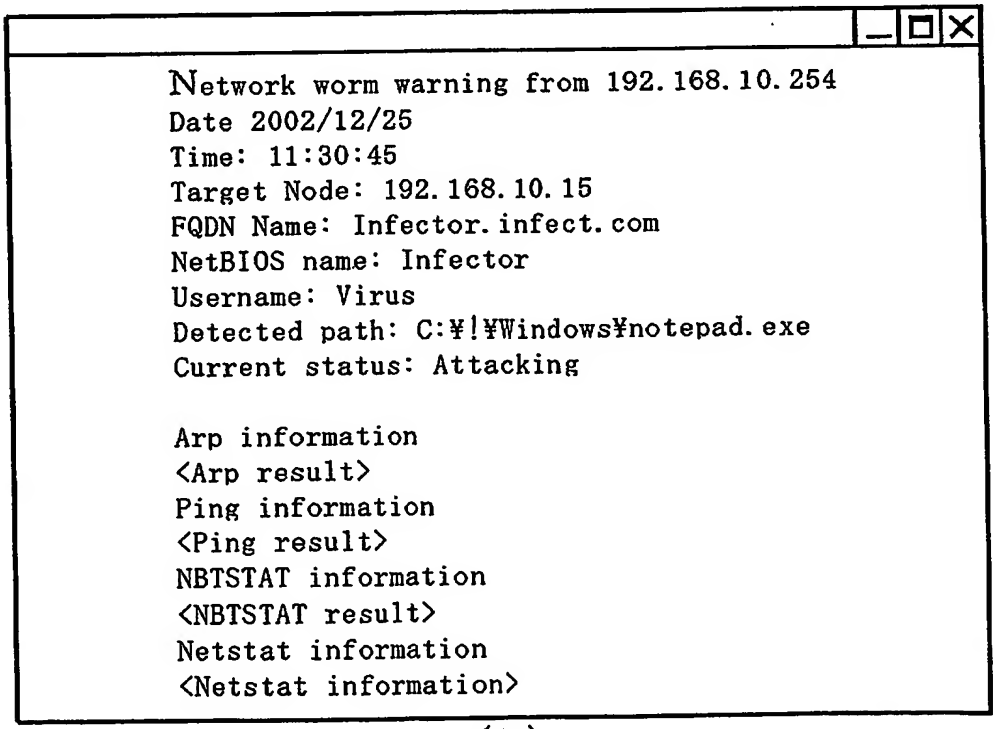

10
監視
コンピュータ
12
1
1
13
おとり
サーバ
ネットワーク
インタフェース
14
おとり
フォルダ
15
おとり
アプリケーション
2
スピーカ
16
通信情報解析手段
警報発生
手段
19
ディスプレイ
3
送信元ＩＰアドレス
8
17
18
コンピュータ攻撃手段
検出報告送信手段
I／F
6
4
5
ウィルス
7

図2


Network worm warning from 192.168.10.254
Date 2002/12/25
Time: 11:30:45
Target Node: 192.168.10.15
FQDN Name: Infector.infect.com
NetBIOS name: Infector
Username: Virus
Detected request: /default.ida?NNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3
%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090
%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
Current status: Attacking
Arp information
<Arp result>
Ping information
<Ping result>
NBTSTAT information
<NBTSTAT result>
Netstat information
<Netstat information>

(a)


Network worm warning from 192.168.10.254
Date 2002/12/25
Time: 11:30:45
Target Node: 192.168.10.15
FQDN Name: Infector.infect.com
NetBIOS name: Infector
Username: Virus
Detected path: C:¥!¥Windows¥notepad.exe
Current status: Attacking
Arp information
<Arp result>
Ping information
<Ping result>
NBTSTAT information
<NBTSTAT result>
Netstat information
<Netstat information>

(b)

図3

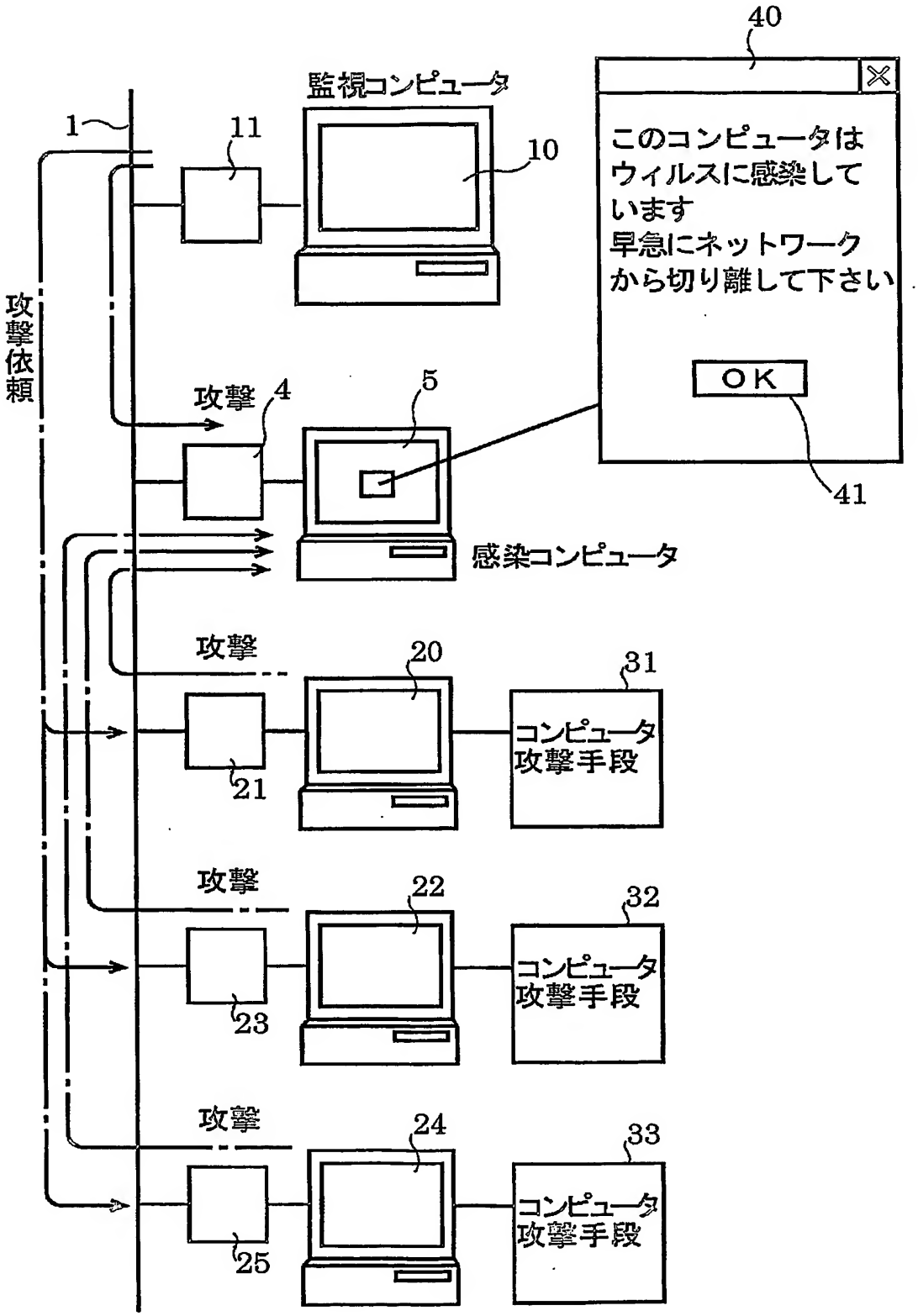

40
監視コンピュータ
1
11
10
このコンピュータは
ウィルスに感染して
います
早急にネットワーク
から切り離して下さい
攻撃依頼
攻撃
4
5
OK
41
感染コンピュータ
攻撃
20
31
コンピュータ
攻撃手段
21
攻撃
22
32
コンピュータ
攻撃手段
23
攻撃
24
33
コンピュータ
攻撃手段
25

図4

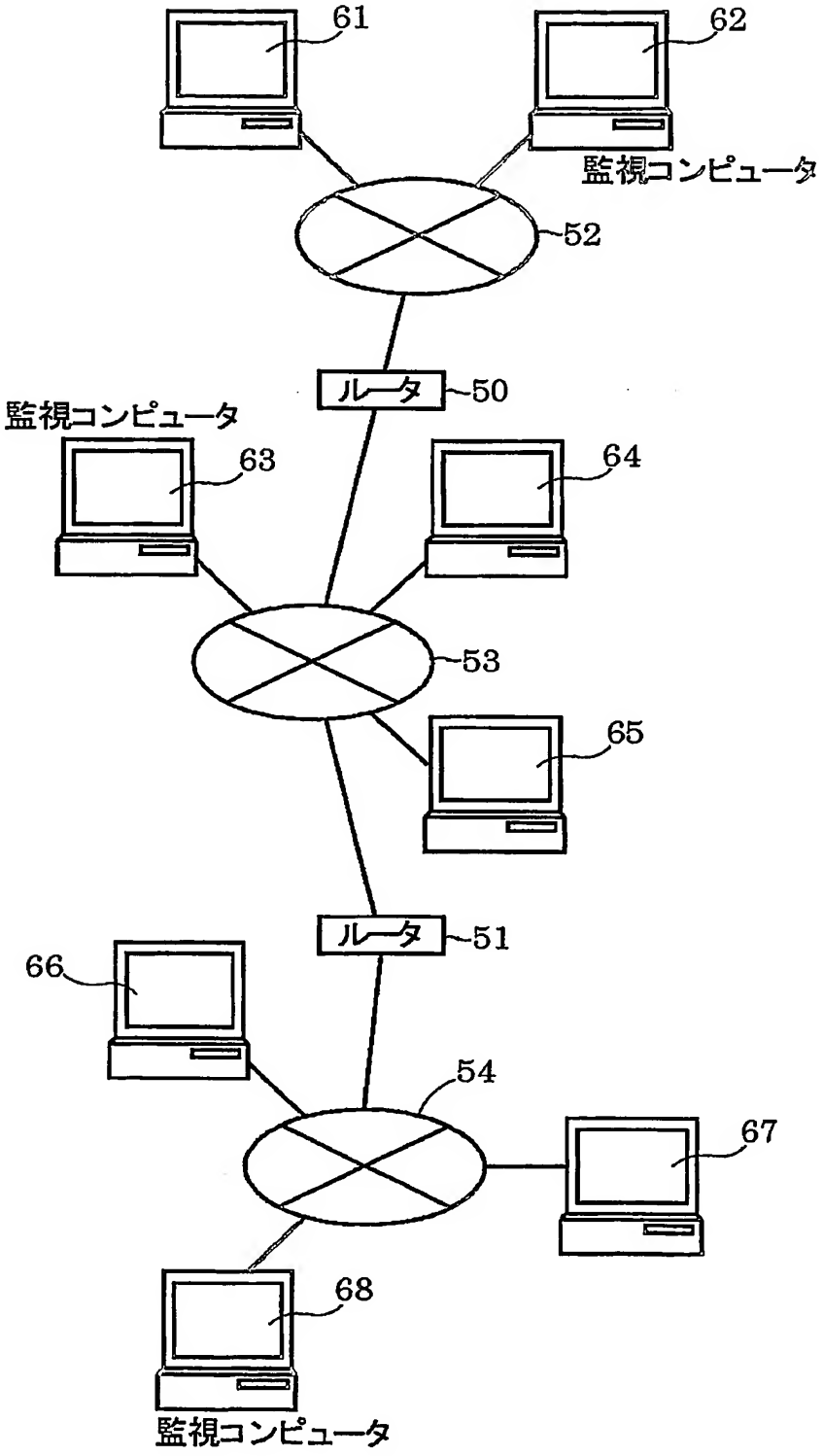

61
62
監視コンピュータ
52
ルータ
50
監視コンピュータ
63
64
53
65
ルータ
51
66
54
67
68
監視コンピュータ

図5

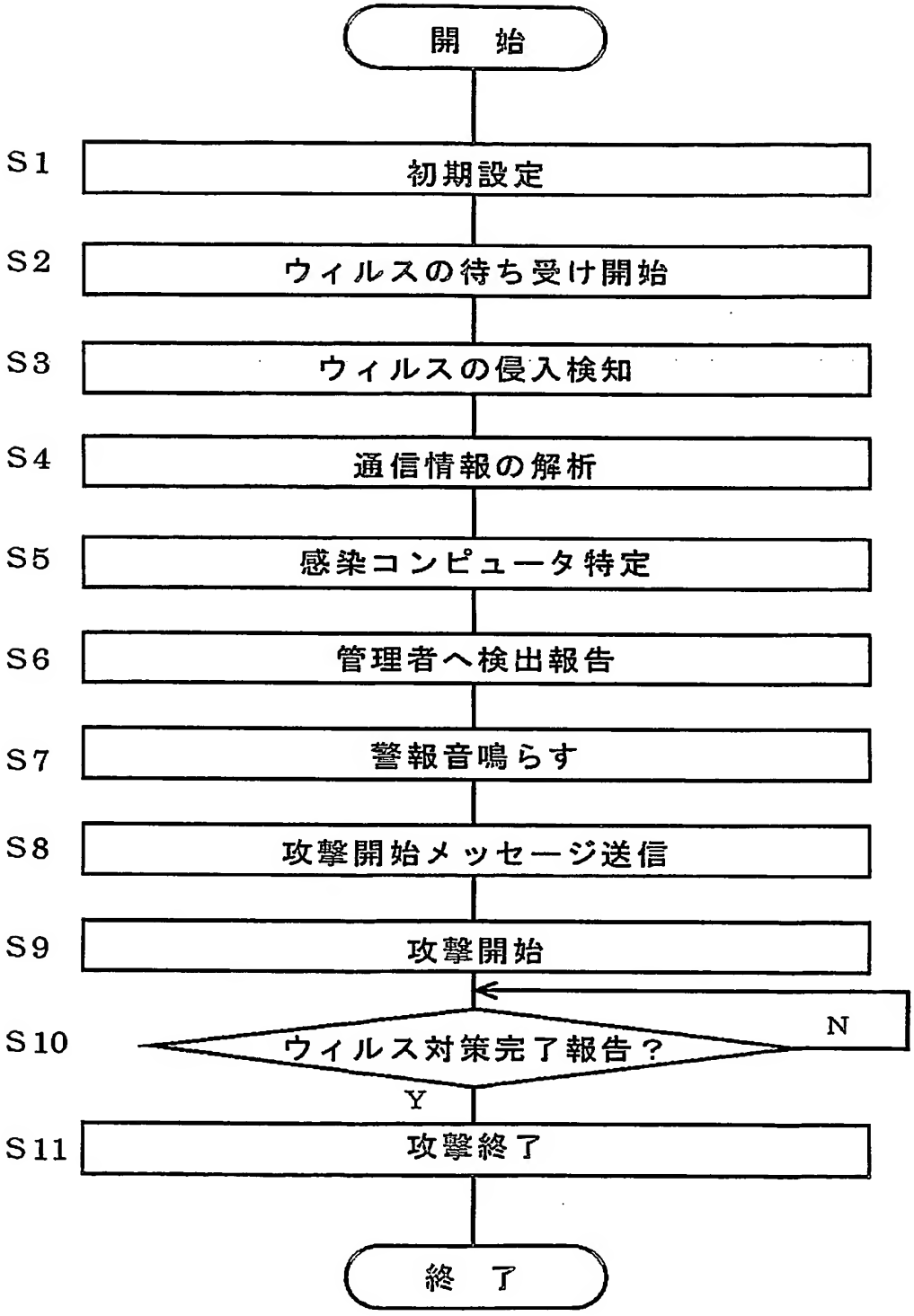
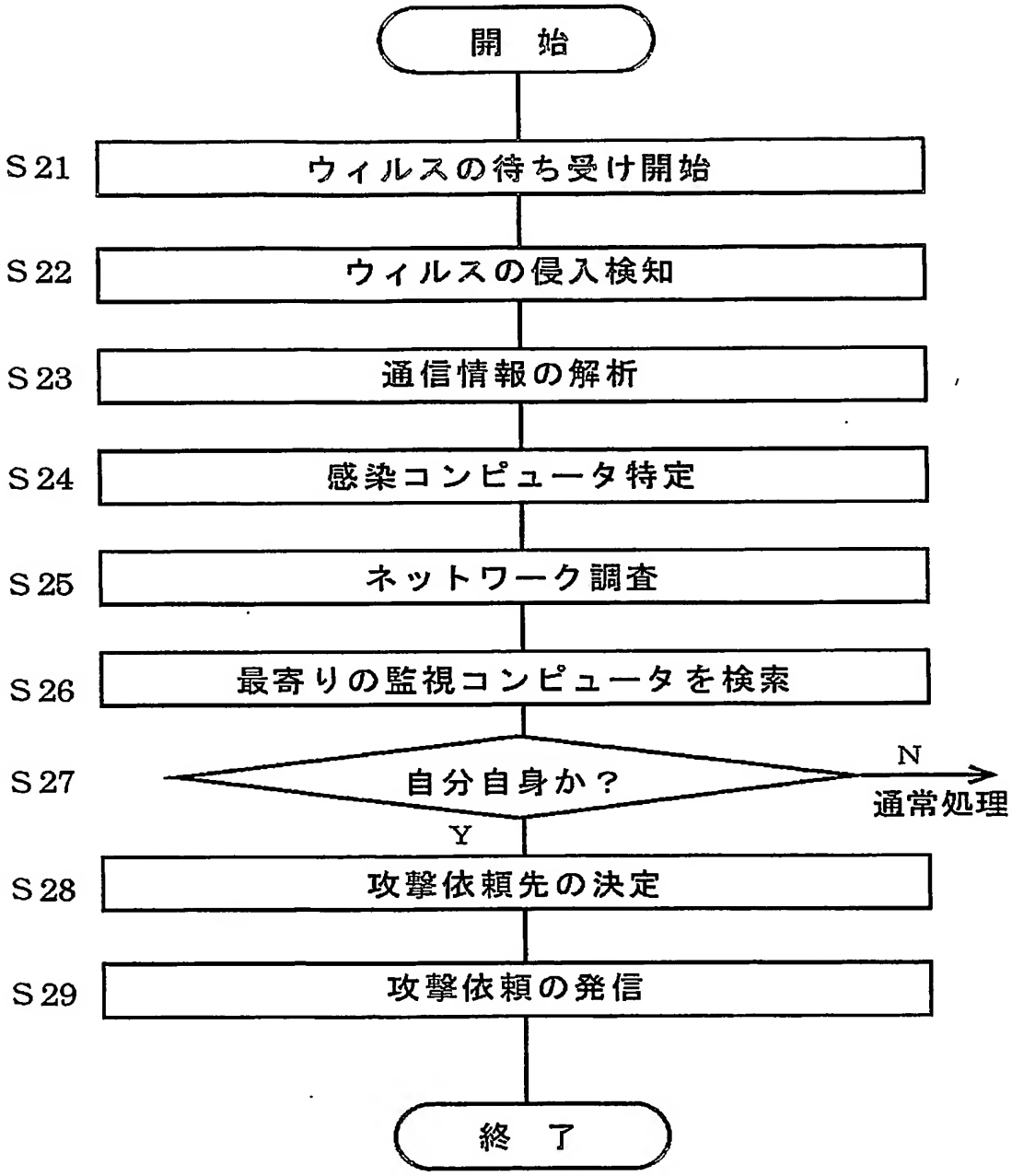

開　始
S1
初期設定
S2
ウィルスの待ち受け開始
S3
ウィルスの侵入検知
S4
通信情報の解析
S5
感染コンピュータ特定
S6
管理者へ検出報告
S7
警報音鳴らす
S8
攻撃開始メッセージ送信
S9
攻撃開始
S10
ウィルス対策完了報告？
N
Y
S11
攻撃終了
終　了

図6


開　始
S21
ウィルスの待ち受け開始
S22
ウィルスの侵入検知
S23
通信情報の解析
S24
感染コンピュータ特定
S25
ネットワーク調査
S26
最寄りの監視コンピュータを検索
S27
自分自身か？
N
通常処理
Y
S28
攻撃依頼先の決定
S29
攻撃依頼の発信
終　了

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/003520

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F9/06, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

| | | | |
|---|---|---|---|
| Jitsuyo Shinan Koho | 1922-1996 | Toroku Jitsuyo Shinan Koho | 1994-2004 |
| Kokai Jitsuyo Shinan Koho | 1971-2004 | Jitsuyo Shinan Toroku Koho | 1996-2004 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | WO 2002/006928 A (VCIS Inc.), 24 January, 2002 (24.01.02), Full text; Figs. 1 to 6 | 1-10,12,13, 16-19 |
| A | Full text; Figs. 1 to 6 & JP 2004-504662 A | 11,14,15 |
| Y | "Naze Konna Seihin ga Nai no daro", Computer & Network LAN, Vol.17, No.12, (Japanese), Ohmsha, Ltd., 01 December, 1999 (01.12.99), pages 45 to 47 | 1-10,12,13, 16-19 |
| A | pages 45 to 47 | 11,14,15 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| | |
|---|---|
| Date of the actual completion of the international search<br>15 April, 2004 (15.04.04) | Date of mailing of the international search report<br>11 May, 2004 (11.05.04) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (January 2004)

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2004/003520

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 2002-252654 A (Mitsubishi Electric Corp.), 06 September, 2002 (06.09.02), Full text; Figs. 1 to 28 (Family: none) | 3-5,8-10, 16,17,19 |
| A | JP 2002-73433 A (Mitsubishi Electric Corp.), 12 March, 2002 (12.03.02), Full text; Figs. 1 to 7 (Family: none) | 1-19 |
| A | JP 2003-36243 A (KDDI Corp.), 07 February, 2003 (07.02.03), Full text; Figs. 1 to 11 (Family: none) | 1-19 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００３５２０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷ Ｇ０６Ｆ９／０６，Ｇ０６Ｆ１５／００

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷ Ｇ０６Ｆ９／０６，Ｇ０６Ｆ１５／００

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | １９２２－１９９６年 |
| 日本国公開実用新案公報 | １９７１－２００４年 |
| 日本国登録実用新案公報 | １９９４－２００４年 |
| 日本国実用新案登録公報 | １９９６－２００４年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Ｙ | ＷＯ　２００２／００６９２８　Ａ（ヴィースィーアイエス　インコーポレイテッド）<br>２００２．０１．２４，<br>全文，第１－６図 | 1-10, 12, 13, 16-19 |
| Ａ | 全文，第１－６図<br>＆ＪＰ　２００４－５０４６６２　Ａ | 11, 14, 15 |

[x] Ｃ欄の続きにも文献が列挙されている。　　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

| | |
|---|---|
| 国際調査を完了した日<br>１５．０４．２００４ | 国際調査報告の発送日　11.5.2004 |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 特許庁審査官（権限のある職員）　５Ｂ　９４６３<br>後藤　和茂<br>電話番号　０３－３５８１－１１０１　内線　６９１６ |

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００３５２０

Ｃ（続き）．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Ｙ | なぜこんな製品がないのだろう，コンピュータ＆ネットワークＬＡＮ，第１７巻　第１２号，（日），株式会社オーム社，１９９９．１２．０１，第４５－４７頁 | 1-10，12，13，16-19 |
| Ａ | 第４５－４７頁 | 11，14，15 |
| Ｙ | ＪＰ　２００２－２５２６５４　Ａ（三菱電機株式会社）２００２．０９．０６，全文，第１－２８図（ファミリーなし） | 3-5，8-10，16，17，19 |
| Ａ | ＪＰ　２００２－７３４３３　Ａ（三菱電機株式会社）２００２．０３．１２，全文，第１－７図（ファミリーなし） | １－１９ |
| Ａ | ＪＰ　２００３－３６２４３　Ａ（ケイディーディーアイ株式会社）２００３．０２．０７，全文，第１－１１図（ファミリーなし） | １－１９ |